Duke Data Risk Assessment (DDRA)

Introduction
We all appreciate the amazing opportunities that information technology (IT) offers Duke to better serve our teaching, research, and service mission. As a complex and dynamic organization, Duke has launched new IT applications and created systems that enable faculty, staff, and students to learn more efficiently and effectively.

Information technology also creates risk -- one prominent area of risk is the difficulty of understanding and addressing internal and external threats to confidential, personal or proprietary data that, if compromised, could cause significant harm to individuals or to Duke. Consider some of the types of harm that can result from failure to adequately protect confidential data:

- Identity Theft
- Disruption of Operations / Services
- Legal Liability
- Damage to University Reputation
- Regulatory Fines

Federal and state law, industry practices, and principles of data stewardship have all driven home the fact that individuals who create, use, or maintain Sensitive or Restricted university data are responsible for adequate protection of that data. The Duke Data Risk Assessment program (DDRA) is a resource to help each school, department, or organizational group better understand what threatens the data in its computing environment, where the greatest vulnerabilities exist, and what safeguards can be implemented. The DDRA tool offers suggestions for what safeguards may be appropriate in order to mitigate the most common threats and provides a reporting template to help synthesize the learning and proposed changes that result from the DDRA process.

It is important to note that DDRA is not a mandate that requires that all mitigation strategies be implemented. Rather, it is a roadmap to help organizations identify areas of risk and select appropriate strategies and timeframes to mitigate those risks.

How do we complete the process?
DDRA is broken out into five basic steps:

- Step 1: Develop an inventory of systems and services utilized by the department. Refer to the Duke Data Classification Standard for data classification options. Remember to include applications, databases, operating systems, electronic storage.

Perform steps 2-4 for each inventory item classified as sensitive or restricted per the Duke Data Classification Standard:

- Step 2: Identify safeguards in place for each of the seven common threats listed in the Threat Assessment spreadsheet.
- Step 3: Assign a probability level and consequence level to each threat based on the safeguards in place.
- Step 4: Identify the safeguards you plan to implement in the future to better secure departmental data.
- Step 5: Issue the Executive Summary indicating risks to data security for your environment and action plans to implement future safeguards.

What if I don’t like everything about the process?
DDRA is a tool for Duke University Departments to meet their responsibility of reasonably protecting sensitive and restricted data. DDRA can be tailored to fit the needs or wishes of any organization.

Customization opportunities are available for departments; each organization may modify the tool as needed to meet the basic objective of understanding what data exists, evaluating current protections, and taking
appropriate steps to mitigate priority risks. For example, if an organization manages several applications on the same server and under the same conditions, the organization may group them into a single assessment.

What if I need help?
The University IT Security Office is available to assist you with any aspect of the DDRA process. If you have questions, please write to security@duke.edu.

Reporting Process
During step 5 noted above, the executive summary for the organization, signed by the Business Manager and the IT Director, should be reported to:

• The University’s IT Security Office and
• The Office of Internal Audits

The purpose of the reporting is to:
1. Ensure that the organization understands where protected university data resides, the risks involved with regard to such data, and safeguards to help mitigate the risks.
2. Provide an opportunity for organization IT and business leadership to review the assessment and provide feedback.
3. Provide central IT and other leadership the ability to learn about trends in risks and solutions and to identify when a central solution might be appropriate.

Updates
Because our data and IT needs may vary throughout the years, we must track changes to evaluate needs for further protections over our sensitive and restricted data. An updated Executive Summary should be issued annually. Tracking information should be updated as needed to support the DDRA coordinators in the organization, and need not be submitted under the reporting process outlined above.

INSTRUCTIONS FOR DDRA PROGRAM

Preparation Stage
The efficiency and effectiveness of this program hinge largely on the initial planning and preparation that take place. For example, Step 1 calls for development of a complete inventory of applications and databases within the organization. In order to develop this inventory efficiently and accurately, it is crucial to have the right team in place. Depending on the size of the organization, this could mean including on the team the two or three individuals most familiar with operations and information systems in the organization, or forming a much larger team that reports information to a single project coordinator. Good planning in the team formation stage can avert significant lost time, and lead to more complete results.

In view of the importance of sound preparation, a summary of organizational approach form has been developed to provide guidance for the program initiation steps.

STEP 1: Inventory

Name Your Organization
Using the Inventory Worksheet, start by identifying your school, center, department, institute, or other organization at the upper left corner of the sheet. You may break this up at whatever organizational level you feel appropriate for your area. Then prepare to inventory your applications and databases.

Inventory Your Applications & Databases – Create the List
The inventory of applications/databases is the first major task and provides the basis for identifying where to conduct your risk assessment. The purpose of the inventory process is to make sure all systems containing protected university data are identified and scheduled for a detailed risk assessment.

Protected university data includes all data classified as Sensitive or Restricted as defined in the Duke Data Classification Standard.

The scope should include applications and databases containing protected university data that your organization is directly responsible for designing, managing, administering or operating. This may include data sets that are stored on individual desktops, laptops, or other portable devices and is not limited to large, more centrally-supported applications and databases.

As for central systems, organizations will not generally be responsible for listing or assessing university-wide applications and databases containing protected university data that the organization is not responsible for designing, managing, administering, or operating. However, if your organization extracts data from these systems and manages that data in local databases, include those in your inventory.

In the column headed “Application/Database Name,” provide a name for the application or database. This may be an acronym or a few words that describe a computer system through which data is created, stored, and retrieved to support a business function.

**Description of Each Application or Database**

In the column headed “Describe Information,” provide some additional detail about the type of information being processed, received, stored, or transmitted. For example, is it personal health information such as medications, test results, diagnosis, appointments, or other confidential data such as Social Security, credit card, employment, contact information, biometric, GPS location? Is it mission critical information such as emails, budget/finance records, or time and attendance data?

In the columns under the heading “Where is the information?,” indicate the media used to receive, store, or transmit the information. Simply enter an “X” under the appropriate media description. If you select “Other Portable or Wireless Device,” or “Other Electronic Media,” describe the media under “Describe Information” (see preceding paragraph) if you think this may be useful later when completing the detailed risk assessment.

In the column headed “Describe the source of the data,” describe the source specifically (e.g., other department/operating units, university central system, an external business associate, vendor).

In the column headed “With whom is the data shared?,” describe the destination of the information in specific detail (e.g., other department/operating units, external business associates, vendors).

In the column headed “Estimate the volume of data,” estimate the volume of data based on the subject of the data (i.e. number of students, patients, employees, faculty, research subjects). This is important from the perspective of prioritizing your risk assessment and mitigation activities. Use whatever quantifiable measures you think best apply. Again, this is intended to help you focus your efforts on the greatest areas of vulnerability so use it only to the extent it provides you with that perspective.